BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of The original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
Please do not report the images to the
Image Problem Mailbox.**

7

AF

9) (11) Publication number: 200

Generated Document.

PATENT ABSTRACTS OF JAPAN

21) Application number: **10296522**

22) Application date: **19.10.98**

(51) Intl. Cl.: **H04L 12/56** H04L 12/40

(30) Priority:

(43) Date of application publication: **28.04.00**

84) Designated contracting states:

(71) Applicant: **NEC CORP**

(72) Inventor: **HASHIMOTO JUNJI**

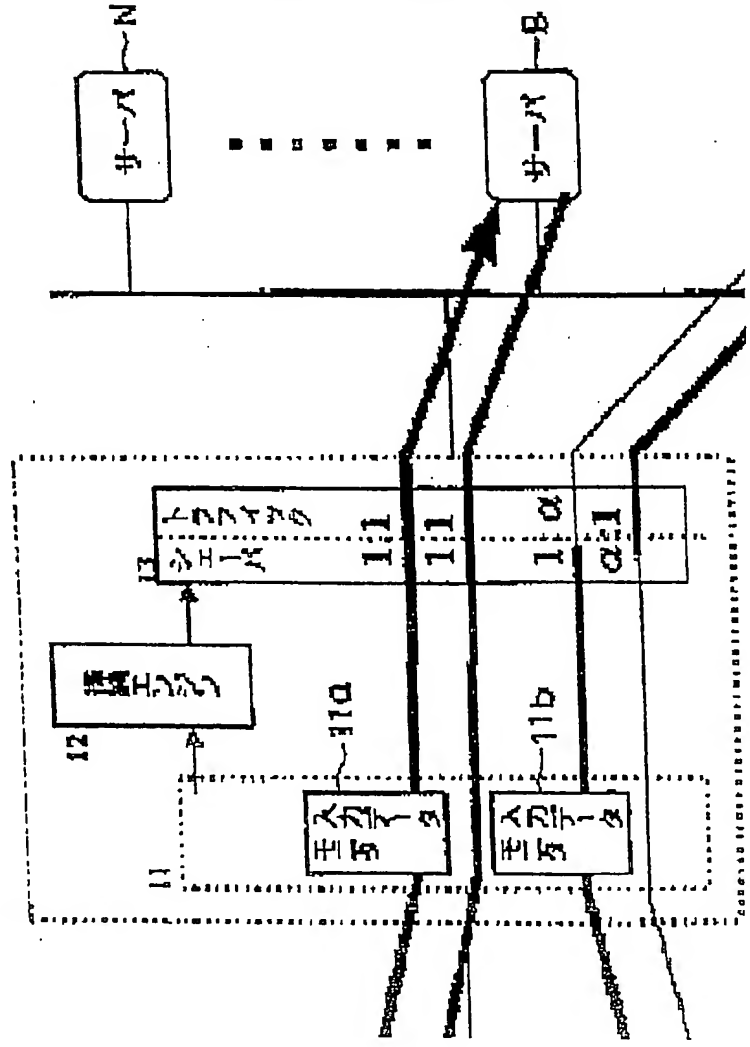
(74) Representative:

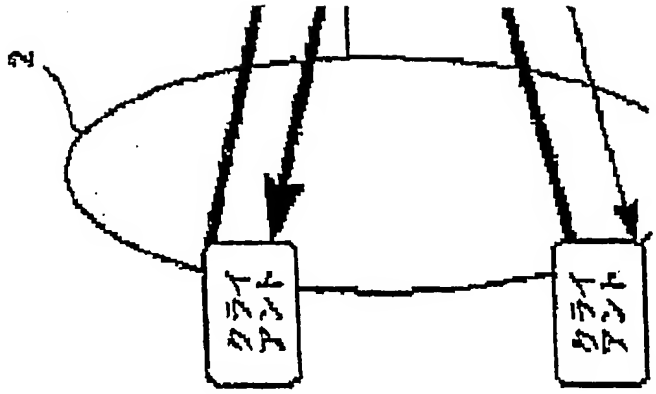
(54) NETWORK ATTACK PROTECTION SYSTEM FOR TRAFFIC SHAPING

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a network attack protection ystem which can be effective to the attack by a scanner attacking totally, can unnecessitate the change of a server program and can quickly respond to the contents of the attack.

SOLUTION: Communication data transmitted from an external network 2 are sampled by input data monitors 11a and 11b. When an inference engine 12 detects matching between the pattern of communication data sampled by these input data monitors 11a and 11b and an attack pattern stored in the inference engine 12, the rate α of shaping traffic with a traffic shaper 3 is controlled.




2
ダイアフラム
ダイアフラム

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－124955
（P2000－124955A）
(43)公開日　平成12年４月28日(2000.4.28)

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
H04L 12/56		H04L 11/20	102E	5J104
12/40		H04K 3/00		5K030
// H04K 3/00		H04L 11/00	320	5K032

審査請求 有　請求項の数5　OL　（全５頁）

(21)出願番号　特願平10－296522

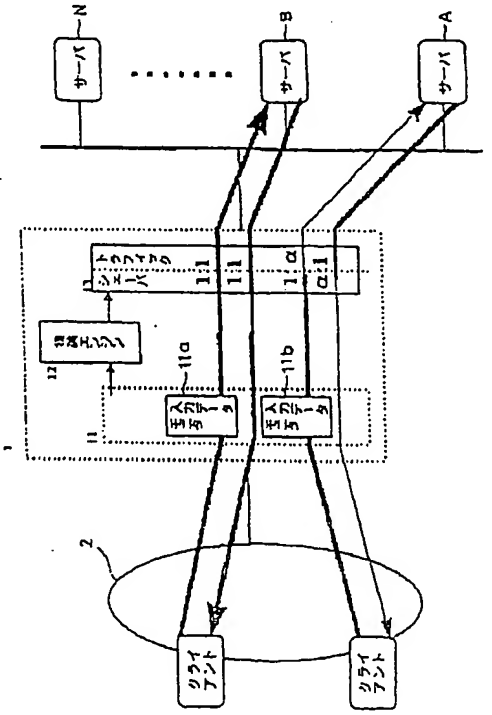
(22)出願日　平成10年10月19日(1998.10.19)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　橋本　淳二
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100089875
弁理士　野田　茂

Ｆターム(参考)　5J104 AA12 AA41 PA07
5K030 GA15 HC01 HC14 LC02 LC11
5K032 AA08 CC05 EA06

(54)【発明の名称】　トラフィックシェーピングによるネットワークアタック防御システム

(57)【要約】
【課題】　網羅的にアタックをかけるスキャナなどの攻撃に有効、かつサーバプログラムの変更を不要にでき、アタックの内容に即応できるトラフィックシェーピングによるネットワークアタック防御システムを提供すること。
【解決手段】　入力データモニタ１１ａ，１１ｂにより外部ネットワーク２から伝送される通信データを採取する。この入力データモニタ１１ａ，１１ｂで採取した通信データのパターンと推論エンジン１２に記憶されているアタックパターンとがマッチングしていることを推論エンジン１２で検出すると、トラフィックシェーパ１３によりトラフィックをシェーピングする割合αを制御する。



【特許請求の範囲】
【請求項１】　外部ネットワークからの通信データを採取する入力データモニタと、
コンピュータへのアタックパターンがあらかじめ記憶され、上記入力データモニタより採取された上記通信データのパターンを検出して、その検出した上記通信データのパターンが上記記憶したアタックパターンとのマッチングの有無により上記通信データが上記コンピュータへのアタックであるか、否かの判断をする推論エンジンと、
上記推論エンジンが上記通信データのパターンから上記コンピュータへのアタックパターン検出時にトラフィックをシェーピングする割合を制御するトラフィックシェーパと、
を備えることを特徴とするトラフィックシェーピングによるネットワークアタック防御システム。
【請求項２】　上記トラフィックシェーパは、上記推論エンジンによる上記通信データのパターンと上記アタックパターンのマッチング検出時にトラフィックをシェーピングする割合αを既定値（０＜α＜１）とすることを特徴とする請求項１記載のトラフィックシェーピングによるネットワークアタック防御システム。
【請求項３】　上記トラフィックシェーパは、上記推論エンジンによる上記通信データのパターンと上記アタックパターンのマッチング検出時にクライアントからサーバへのデータをα倍にすることを特徴とする請求項１記載のトラフィックシェーピングによるネットワークアタック防御システム。
【請求項４】　上記トラフィックシェーパは、上記推論エンジンによる上記通信データのパターンと上記アタックパターンのマッチング検出時にサーバからクライアントへのトラフィック量をα倍にすることを特徴とする請求項１記載のトラフィックシェーピングによるネットワークアタック防御システム。
【請求項５】　上記トラフィックシェーパは、上記推論エンジンにより検出したアタックの発信元である上記通信データが終了するとトラフィックをシェーピングする割合αを元の既定値（０＜α＜１）に戻すことを特徴とする請求項１記載のトラフィックシェーピングによるネットワークアタック防御システム。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、トラフィックのシェーピングを行い、次のホストコンピュータ（以下、ホストと略称する）へのアタックへの移行時間を引き延ばすことにより、他のホストへのアタック時間を引き延ばすことができ、ホストへのアタックの解析が可能になり、アタックする犯人を特定するための情報を得ることができるようにしたトラフィックシェーピングによるネットワークアタック防御システムに関する。
【０００２】
【従来の技術】インターネットなどのパブリックネットワークの普及に伴い、ネットワーク経由による情報の盗難や不正利用などの犯罪が急増している。インターネットでは、不正アクセスのためのプログラムが流通しており、網羅的にアタックし、セキュリティホールを発見しようとするツールが数多く存在する。現在、これらのアタッキングツールやアタッカへの対策が急務であり、その対策に種々の試みがなされている。
【０００３】たとえば、特開平０２-３０２１３９号公報には、複数のネットワーク間の接続部に通信データの発信先アドレスと発信元アドレスをチェックし、アクセス権を記録した内容にしたがって、不正アクセスを遮断する不正アクセス防止手段を備えたネットワークセキュリティが開示されている。
【０００４】また、ＬＡＮあるいは公衆網などの伝送媒体に構築されるネットワークシステムにおいて、管理装置がアラーム情報と各中継装置が有するアクセス履歴情報とから不正アクセスをした端末装置が各中継装置のどちら側のポートに接続されているかを絞り込んでいくことにより、不正アクセスをした端末装置がどのＬＡＮ上で接続されているかを特定するセキュリティ方式が開示されている。
【０００５】
【発明が解決しようとする課題】しかしながら、これらの公報の場合には、いずれもホストへのアタックに対する直接的な対策とはならない。このような従来のネットワークアタック防御システムの課題を挙げると、以下のごとくである
【０００６】すなわち、従来は網羅的にインターネット上のサーバに対して「ポートスキャン」などを行われた場合、パケットフィルクリングなどにより、これらのアクセスを「遮断する」アイデアは存在した。しかし、この場合、アクセスを遮断することは即座に次のアタックに切り替わるきっかけとなってしまうことが多いため、アタッカは短時間でサービスポートなどを検出することができ、かつ迅速に次のアタックへ移行することができてしまうという課題がある。
【０００７】また、従来のアタックを遮断する方法もあるが、この方法では、攻撃元とのコネクションがすぐに切れてしまうことになり、攻撃元が次にどんなアタックを行うかを予想することが難しいという課題がある。
【０００８】この発明は、上記従来の課題を解決するためになされたもので、サーバ１台当たりのアタック時間を長くすることができ、網羅的にアタックをかけるスキャナなどの攻撃に有効かつ、サーバプログラムの変更を不要にでき、サーバに検出モジュールの導入を不要にできるとともに、アタックの内容に即した対応が可能となるトラフィックシェーピングによるネットワークアタック防御システムを提供することを目的とする。

【０００９】
【課題を解決するための手段】上記目的を達成するために、この発明によるトラフィックシェーピングによるネットワークアタック防御システムは、外部ネットワークからの通信データを採取する入力データモニタと、コンピュータへのアタックパターンがあらかじめ記憶され、上記入力データモニタより採取された上記通信データのパターンを検出して、その検出した上記通信データのパターンが上記記憶したアタックパターンとのマッチングの有無により上記通信データが上記コンピュータへのアタックであるか、否かの判断をする推論エンジンと、上記推論エンジンが上記通信データのパターンから上記コンピュータへのアタックパターン検出時にトラフィックをシェーピングする割合を制御するトラフィックシェーパとを備えることを特徴とする。
【００１０】この発明によれば、入力データモニタにより外部ネットワークから伝送される通信データを採取すると、この採集された通信データのパターンを推論エンジンにより検出される。検出された通信データのパターンが推論エンジンであらかじめ記憶されているコンピュータへのアタックパターンとのマッチングの有無を検出し、その検出の結果、アタックパターンと通信データのパターンがマッチングしていると判断すると、トラフィックシェーパにより、トラフィックをシェーピングする割合αを制御する。
【００１１】したがって、この発明では、サーバ１台当たりのアタック時間を長くすることができ、網羅的にアタックをかけるスキャナなどの攻撃に有効かつ、サーバプログラムの変更を不要にでき、サーバに検出モジュールの導入を不要にできるとともに、アタックの内容に即した対応が可能となる。
【００１２】
【発明の実施の形態】以下、この発明によるトラフィックシェーピングによるネットワークアタック防御システムの実施の形態について図面に基づき説明する。図１はこの発明の第１実施の形態の構成を示すブロック図である。この図１において、この第１実施の形態は防御装置１を備えている。クライアントX，Yとコンピュータとしてのサーバ A，B，・・Nには特別な仕組みは必要ない。
【００１３】防御装置１は、外部ネットワーク２からの通信データを採取する入力データモニタ１１ａ、入力データモニタ１１ｂによって得られた通信データのパターンを検出し、アタックかどうかを判断する推論エンジン１２と、トラフィックをシェーピングする割合を制御するトラフィックシェーパ１３とにより構成される。推論エンジン１２はあらかじめアタックパターンを記憶しており、推論エンジン１２により入力データモニタ１１ａ、入力データモニタ１１ｂによって検出された通信データのパターンとアタックパターンがマッチングしていることを検出することにより、アタックを検出する。トラフィックシェーパはアタック検出時にトラフィックをシェーピングする割合α（０＜α＜１）を記憶している。
【００１４】次に、以上のように構成されたこの第１実施の形態の動作について図２のフローチャート沿って説明する。図２のステップＳ１では、外部ネットワーク２を通してクライアントX、クライアントYから伝送される通信データが入力データモニタ１１ａ，１１ｂによって採取される。この入力データモニタ１１ａ，１１ｂによって採取された通信データは推論エンジン１２で検出される。
【００１５】この推論エンジン１２には、あらかじめサーバA～Nへのアタックパターンが記憶されており、推論エンジン１２が入力データモニタ１１ａ，１１ｂによって採取された通信データを検出すると、その検出した通信データのパターンとアタックパターンとのマッチングの有無を検出する。この際、入力データモニタ１１ａ，１１ｂによって採取された通信データからアタックパターンらしい通信データが検出されるまで上ステップＳ１の処理の実行を繰り返す。
【００１６】推論エンジン１２は、入力データモニタ１１ａ，１１ｂによって採取された通信データの検出中に、この通信データのパターンがアタックパターンにマッチングすることを検出すると、ステップＳ２で推論エンジン１２はトラフィックシェーパ１３に対して、アタックパターンが検出されたことを通知する。トラフィックシェーパ１３は、この通知を受けると、トラフィックをα倍にシェーピングする。
【００１７】このシェーピングする状態は、図１におけるクライアントYからサーバAへのアクセスがこれに当たる。このトラフィックシェーパ１３はクライアントYからサーバAへの通信データを「１：１」から「１：α」倍に、また同様にサーバAからクライアントYへのトラフィックを「１：α」から「α：１」倍にする。推論エンジン１２により検出されたトラフィックが継続している場合であることをステップＳ３で推論エンジン１２が検出すると、ステップＳ４でトラフィックシェーパ１３はトラフィックの割合を減少するか、否かの判断を行い、トラフィックシェーパ１３はトラフィックの割合を減少させない場合には、再びステップＳ３の処理に戻る。
【００１８】また、ステップＳ４において、トラフィックシェーパ１３はトラフィックの割合を変更する場合（減少させる場合）には、ステップＳ５において、既定のトラフィックの割合（０＜α＜１）を変更して、ステップＳ２の処理に戻る。一方、上記ステップＳ３において、推論エンジン１２は検出したアタックの発信元からの通信データが終了したことを検出すると、ステップＳ６で推論エンジン１２はトラフィックのシェーピングを

既定値（０＜α＜１）に戻す。

【００１９】

【発明の効果】以上のように、この発明によれば、通信データとあらかじめ推論エンジンに記憶されたアタックパターンとの一致の検出時に、トラフィックシェーピングによってアタックのトラフィックを減少させるようにしたので、コネクションの保持時間を長くし、サーバ１台あたりのアタック時間を増加させることができ、１台あたりのアタック時間を増加させることは、網羅的にアタックをかけるスキャナなどの攻撃に有効である。また、サーバプログラムを変更する必要がなくなり、一箇所で集中的にアタックの検出を行うため、それぞれのサーバに検出モジュールを導入する必要がなくなる。さらに、シェーピングによる時間稼ぎを行うことで、サーバのログから時間的余裕を持ってアタックの内容を見ることができ、これにより、アタックの内容に即した対応が可能となる。

【図面の簡単な説明】

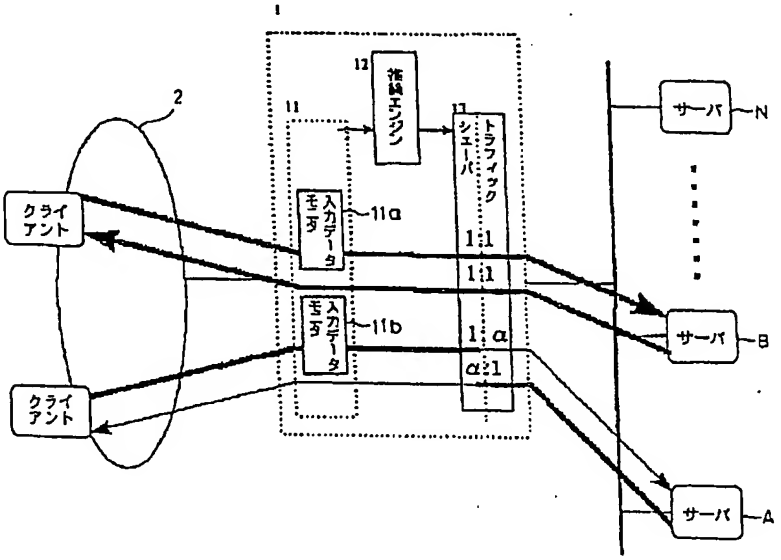
【図１】この発明によるトラフィックシェーピングによるネットワークアタック防御システムに第１実施の形態の構成を示すブロック図である。

【図２】図１のトラフィックシェーピングによるネットワークアタック防御システムの動作を説明するためのフローチャートである。

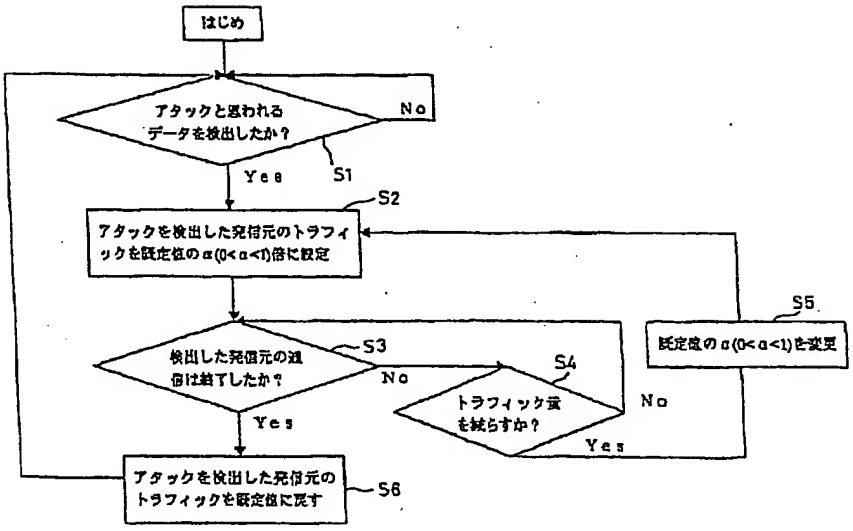
【符号の説明】

１……防御装置、２……外部ネットワーク、１１ａ，１１ｂ……入力データモニタ、１２……推論エンジン、１３……トラフィックシェーパ、Ａ～Ｎ……サーバ、Ｘ，Ｙ……クライアント。

【図１】



【図２】


はじめ
アタックと思われるデータを検出したか？
No
Yes
S1
S2
アタックを検出した発信元のトラフィックを既定値のα(0<α<1)倍に設定
S3
検出した発信元の通信は終了したか？
No
Yes
S4
トラフィック量を減らすか？
No
Yes
S5
既定値のα(0<α<1)を変更
アタックを検出した発信元のトラフィックを既定値に戻す
S6

(12) Publication of Laid-Open Patent (A)
(19) Japanese Patent Office (JP)
(11) Patent Application Publication No. 2000-124955 (P2000-124955A)

(43) Publication Date: April 28, 2000

---

(51) Int. Cl.[7]	Identifying Symbol	FI		Theme code (reference)
H04 L 12/56		H 04 L 11/20	102E	5J104
12/40		H 04 K 3/00		5K030
// H 04 K 3/00		H 04 L 11/00	320	5K032

Request for Examination: requested
Number of Claims: 5 OL
(Total number of pages in the original Japanese text: 5)

(21) Application Number 10-296522
(22) Application Date: October 19, 1998
(71) Patent Applicant: 000004237
NEC Corp.
5-7-1 Shiba Minato-ku
Tokyo, Japan
(72) Inventor: Junji Hashimoto
NEC Corp.
5-7-1 Shiba Minato-ku
Tokyo, Japan
(74) Patent Agent: Patent Attorney Shigeru Noda (100089875)
F Term (reference) 5J104 AA12 AA41 PA07
5K030 GA15 HC01 HC14 LC02 LC11
5K032 AA08 CC05 EA06

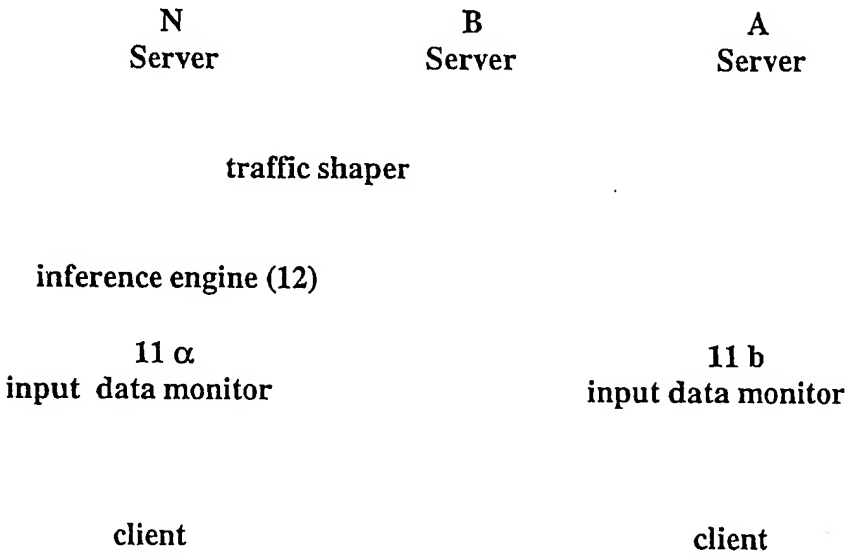
(54) [Title of Invention] Network Attack Control System using Traffic Shaping

(57) Abstract

[Problem to be Resolved] To provide a network traffic attack control system using traffic shaping which is effective in scanning and other types of attack using a network, which eliminates the need to change a server program and which is capable of instantly responding to the contents of the attack.

[Means of Resolving the Problem] Communications data transmitted from an external network 2 is gathered using input monitor 11a and input monitor 11b. When inference engine 12 detects whether or not there is a match between the communications data patterns gathered using these input data monitors 11a and 11b and the attack patterns stored in inference engine 12, it controls the rate α which shapes the traffic using traffic shaper 13.

[captions for diagram on first page]



Specification

[Scope of Patent Claim]
[Claim 1] A network attack control system using traffic shaping which is made up of:

(1) an input monitor which gathers communications data from an external network;

(2) an inference engine in which the attack patterns for the computer have been stored in advance and which detects the aforementioned communications data patterns which have been gathered using the aforementioned input data monitor and which determines whether or not the aforementioned communications data is an attack on the computer by checking to see if the aforementioned communication data patterns which have been detected match with the attack patterns stored; and

(3) a traffic shaper which controls the rate at which the aforementioned inference engine shapes the traffic when the patterns of the attack on the computer are detected from the aforementioned communications data patterns;

[Claim 2] The composition of Claim 1 wherein the aforementioned traffic shaper which makes the rate α--which shapes the traffic when a match between the aforementioned communications data patterns and the aforementioned attack patterns is detected using the aforementioned inference engine--a fixed value ($0 < \alpha < 1$);

[Claim 3] The composition of Claim 1 wherein the aforementioned traffic shaper multiplies by α times the data from the client to the server when a match between the aforementioned communications data patterns and the aforementioned attack patterns is detected using the aforementioned inference engine;

[Claim 4] The composition of Claim 1 wherein the aforementioned traffic shaper multiplies by α times the amount of traffic from the server to the client when a match between the aforementioned communications data patterns and the aforementioned attack patterns is detected using the aforementioned inference engine;

[Claim 5] The composition of Claim 1 wherein the aforementioned traffic shaper returns to the original fixed value ($0 < \alpha < 1$) the rate α which shapes the traffic when the aforementioned communications data which is the source of the attack which has been detected by the aforementioned inference engine is completed.

[Detailed Description of the Invention]
[0001]
[Field of the Invention] The present invention relates to a network attack control system which shapes the traffic, prolongs the time of transition to the next attack on the host computer (hereinafter referred to as "host") so that the time of attack on the other host can be prolonged, the attack on the host can be analyzed and the information which is required to specify the criminal attacker can be obtained.

[0002]
[Description of the Prior Art] In keeping with the dissemination of the Internet and other public networks, theft of information and unauthorized use of the information and other crimes using networks is growing by leaps and bounds. The Internet is becoming flooded with programs used to gain unauthorized access and with tools which attempt to carry out blanket attacks [on the networks] and discover holes in the security are proliferating. Currently there is a strong need for countermeasures which can handle these attack tools and a variety of tests have been carried out for these countermeasures.

[0003] [Japanese] Laid-Open Patent No. 02-302139 discloses a network security [system] which checks the destination address and the source address of the communications data on the connected parts among multiple networks and is provided with a means which is used to prevent unauthorized access and which cuts off unauthorized access according to the contents in which the access authority has been recorded.

[0004] In addition, network systems which are configured in LANs or public networks and other transmission media contain security systems which specify whether or not the terminals which have been granted access without the proper authorization are connected to the LAN by zeroing in on which port of the relay devices the terminals which have been granted unauthorized access are connected to based on the alarm information for the monitoring device and the access history information held by each of the relay devices.

[0005]
[Problems Which the Present Invention Attempts to Resolve] However, when the systems mentioned in the publication were used, none of them were useful as direct countermeasures for handling the attack on the host. The prior-art network attack control systems presented the following problems.

[0006] When "port scanning" and the like were used for the Internet servers comprehensively, there was a concept of "cutting off " access to these using packet filtering and the like. However, in this case, there were problems in that cutting off access oftentimes meant an opportunity [for the attacker] to immediately switch over to the next attack. As a result, the attacker could detect the service port and the like within a short period of time and the attacker could rapidly go to the next attack.

[0007] Although there were prior-art methods of cutting off the attacks, these methods were problematical in that the connection with the attacking source was immediately cut off and the attacker could figure out which [target] he/she could attack next.

[0008] It is an object of the present invention to resolve the problems in the prior art systems mentioned above by providing a network attack control system which is capable of prolonging the attack time per server, which is effective in using scanning and other comprehensive methods to attack the attacker, which eliminates the need to change the server program, which eliminates the need to introduce a detection module to the server and which uses traffic shaping which makes it possible to immediately take care of the contents of the attack.

[0009]
[Means Used to Resolve these Problems] In order to attain the aforementioned objectives, the network attack control system in the present invention is provided with: (1) an input monitor which gathers the communications data from an external network; (2) an inference engine in which the attack patterns for the computer have been stored in advance and which detects the aforementioned communications data patterns which have been gathered using the aforementioned input data monitor and which determines whether or not the aforementioned communications data constitute an attack on the computer by checking to see if there is a match between the aforementioned communication data patterns and the attack patterns stored; and (3) a traffic shaper which controls the rate at which the aforementioned inference engine shapes the traffic when the patterns of the attacks on the computer are detected from the aforementioned communications data patterns.

[0010] In the present invention, when the communications data which have been transmitted from an external network by an input data monitor are gathered, the communication data patterns gathered are detected by the inference engine. The communications data patterns detected determine whether or not there is a match with the patterns of attack on the computer which have been stored in the inference engine beforehand. When it determines that the detection results, the attack patterns and the communications data patterns all match, the rate α which shapes the traffic is thus controlled.

[0011] As a result, when the present invention is used, the attack time per server can be prolonged, the invention is effective in scanning and other types of comprehensive attacks [on computer systems], the need to change the server program is eliminated, the need to introduce a detection module in the server is eliminated and the invention can take care of the contents of the attack itself.

[0012]
[Embodiments of the Present Invention] Next, we shall use diagrams to explain practical embodiments of the network attack control system which uses the traffic shaper in the present invention. Figure 1 is a block diagram of the configuration of the first practical embodiment of the present invention. In Figure 1, the practical embodiment is provided with a control device 1. No special arrangements are required for client X, client Y and for servers A, B .....N as computers.

[0013] The control device 1 is configured of (1) an inference engine 12 which detects the communications data patterns which were obtained by using an input data monitor 11a and an input data monitor 11b which gather communications data from the external network 2 and which determines whether or not there has been an attack; and (2) a traffic shaper 13 which controls the rate at which the traffic is shaped. The inference engine 12 stores the attack patterns beforehand and detects whether or not there is a match with the communications data patterns detected by using input data monitor 11a and input data monitor 11b and the attack pattern itself using the inference engine 12 so that the attack can be detected. The traffic shaper stores the rate α ($0 < \alpha < 1$) which shapes the traffic when an attack is detected.

[0014] Next, we shall use the flowchart in Figure 2 to explain how the practical embodiment which is configured as indicated above operates. In step 1 in Figure 2, the communications data which have been transferred from client X and client Y through the external network 2 is gathered by the input data monitors 11a and 11b. The communications data used by these input data monitors 11a and 11b are detected by the inference engine 12.

[0015] An A ~ N server attack pattern is stored beforehand in this inference engine 12. When the inference engine 12 detects the communications data which are used by input data monitors 11a and 11b, it detects whether or not there is a match between the communications data patterns detected and the attack patterns themselves. At this time, the above-mentioned step S1 is executed repeatedly until attack pattern-like communications data gathered from input data monitors 11a and 11b have been detected.

[0016] When the inference engine 12 detects that there is a match between the communications data patterns and the attack patterns while the communications data gathered using input monitors 11a and 11b are being detected, in Step S 2, the inference engine 12 gives notice that an attack pattern against the traffic shaper 13 has been detected. When the traffic shaper 13 receives this notification, the traffic is shaped by a multiple of α.

[0017] In this shaping mode, access from client Y in Figure 1 to server A corresponds to this. This traffic shaper 13 takes the communications data from client Y to server A and changes them from a multiple of [1 : 1] to a multiple of [1 : α] and likewise takes the traffic from server A to client Y and changes it from a multiple of [1 : α] to a multiple of [α : 1]. In step S 3, when the inference engine 12 detects that the traffic detected using the inference engine 12 is continuing, in step S 4, the traffic shaper determines whether or not the rate of traffic has been reduced. If the traffic shaper 13 has not reduced the rate of traffic, the user must then return to the processing in step 3.

[0018] In addition, if the shape of the traffic has changed (reduced) the rate of traffic in step S4, in step S 5, it changes the fixed rate ($0 < \alpha < 1$) of the traffic and the user must return to the processing in step S 2. Meanwhile, in step S 3 above, when inference engine 12 has detected that the communications data from the attack source address which has been detected has been completed, in step S 6, the inference engine 12 returns the traffic shaping to the fixed value ($0 < \alpha < 1$).

[0019]

[Effectiveness of the Invention]

When the present invention is used and when it has been detected that the communications data and the attack patterns stored in the inference engine beforehand coincide, the attack traffic is reduced by the traffic shaping so that the retention time for the connection can be prolonged and the attacking time per server can be increased. Reducing the attack time per server is effective in scanning and other types of comprehensive attacks [on computer systems]. In addition, the need to change the server program is eliminated and concentrated detection of attacks at a single location can be carried out so that the need to introduce a detection module to the respective serves is eliminated. In addition, by using shaping to gain time, the contents of the attack can be

observed with time to spare from the server log thereby making it possible to handle the contents of the attack.

[Brief Explanation of Figures]

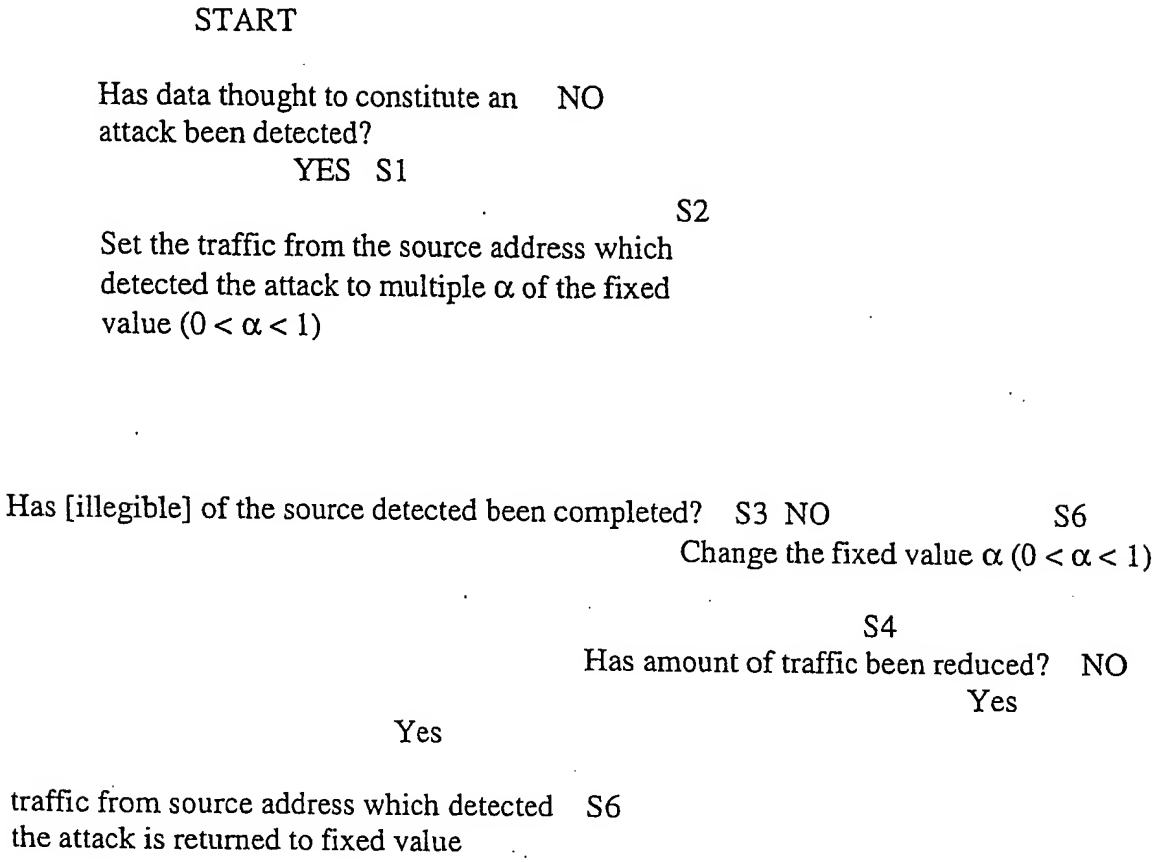
[Figure 1] This is a block diagram of the configuration of the first practical embodiment of the network attack control system using traffic shaping in the present invention.

[Figure 2] This is a flowchart indicating how the network attack control system using the traffic shaping indicated in Figure 1 works.

[Explanation of Numerals]

1.....control device; 2...external network; 11a, 11b...input data monitors; 12...inference engine; 13...traffic shaper; A ~ N....server; X, Y...clients.

[Figure 2]


START
Has data thought to constitute an attack been detected?
NO
YES
S1
S2
Set the traffic from the source address which detected the attack to multiple α of the fixed value (0 < α < 1)
Has [illegible] of the source detected been completed?
S3
NO
S6
Change the fixed value α (0 < α < 1)
S4
Has amount of traffic been reduced?
NO
Yes
Yes
traffic from source address which detected the attack is returned to fixed value
S6